REMARKS

Claims 18-25, 30, and 34-38 are pending in the present application. Claims 1-17, 26-29, and 31-33 are canceled. Claims 18-25, 30, and 34-38 are currently amended. No new matter has been added to currently amended claims 18-25, 30, and 34-38. Claims 18, 30, and 37 are independent.

I. The Prior Art Rejection

Claims 18-30 and 33-38 stand rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 6,279,113 to Vaidya, hereinafter, Vaidya, and further in view of U.S. Patent No. 6,954,765 to Spiegel, hereinafter, Spiegel.

Applicants respectfully traverse these rejections based on the following discussion.

Vaidya discloses a network intrusion detection system (NIDS) for a local network that is based on dynamic signatures comprising packets. The packets may originate from the higher levels of the Open System Interconnection (OSI) model, such as, the application or session layers, or from a lower layer, such as the data link layer.

The present invention describes a method and apparatus for data traffic normalization, in which a traffic normalizer receives packets and packet fragments from an internet and "patches" the packet fragments to eliminate potential conflicts before the packet fragments are transferred to a local network on which NIDS and an end-system reside.

A. The Vaidya Reference

Vaidya discloses a dynamic signature-based network intrusion detection system (IDS) that includes multiple attack signature profiles which are descriptive of identifiable characteristics associated with particular network intrusion attempts associated with network objects located on the network (col. 3, lines 12-16 and cited by the Office Action).

Vaidya also discloses that a simple attack signature profile might provide instructions to

determine if a data packet, which is addressed to a server X for access to application Y, has a source address of user Z. In this example, a network administrator has determined that user Z is not authorized to access application Y on server X. If, upon executing the simple attack profile instructions the virtual processor 36 recognizes that the source address for the data packet is user Z, the virtual processor 36 notifies the reaction module 38, which takes an appropriate action. (col. 7, lines 36-45).

Vaidya further discloses that simple attack signature profiles include only a single expression. In the example above, the expression can be described as "is source address, user Z?" Two other types of attack signature profiles, sequential and timer/counter based, require sequential execution of an instruction or instructions associated with an attack signature profile. (col. 7, lines 46-51).

The sequential attack signature profiles include multiple expressions. For instance, these expressions might include "is source address, user Z?" and "is user Z attempting to access file A?" Instructions associated with the first expression are executed on a first packet associated with an application session to determine that the packet has the user Z source address. However, if this first packet does not include information that user Z is attempting to access file A in application X, a subsequent packet associated with the same application session will have to be analyzed to determine if user Z is attempting to access file A. An entry is made into state cache 44 to indicate that the first expression was satisfied. (col. 7, lines 52-64).

A timer/counter based attack signature profile directs the virtual processor 36 to execute instructions associated with a single expression on every data packet associated with a particular application session to determine whether an event has occurred a threshold number of times within a predetermined time interval. For instance, a timer/counter based attack signature profile might direct the virtual processor 36 to execute an instruction associated with the expression "is user Z attempting to access file A?" on every packet associated with the a session application Y. … The first packet which the virtual processor 36 recognizes as being associated with an attempt by user Z to access file A causes the virtual processor 36 to activate a timer 37 and to set a counter 35 to one. … The timer and counter information are entered into a state cache 44. (col. 8, lines 16-32).

Col. 11, lines 34-51, cited by the Office Action, describe the operation of the state cache 44 in greater detail, which is not necessary for the arguments to be advance below.

To summarize, Vaidya discloses a network intrusion detection system (NIDS) for a local network that is based on dynamic signatures comprising packets. The packets may originate from the higher levels of the Open System Interconnection (OSI) model, such as, the application or session layers, or from a lower layer, such as the data link layer.

The present invention describes a method and apparatus for data traffic normalization, in which a traffic normalizer receives packets and packet fragments from an internet and "patches" the packet fragments to eliminate potential conflicts before the packet fragments are transferred to a local network on which a NIDS and an end-system reside.

Traffic normalization may be required because an NIDS can sometimes be eluded due to certain ambiguities that may arise when observing fragmented network traffic. For example, the IP protocol allows IP packets to be fragmented. Such fragmentation is particularly challenging for an NIDS. For example, suppose that an attacker tries to log in as "root" on a system. To do so, the attacker should send a packet containing "login root." An NIDS can detect this intrusion easily. However, if the packet gets fragmented, it may happen that the attack will span over several packets rather than just one. In this case, the NIDS may, for example, see ten packets containing "l", "o", "g", ... "o", "t". Now suppose that the attacker inserts a packet containing "a" and places it just before the packet containing "r", such that the NIDS receives "login aroot", rather than "login root". The NIDS may not consider "login aroot" to be an attack. With some knowledge of the network topology, however, the attacker may set some of the characteristics (e.g., TIME TO LIVE or maximum transfer unit (MTU) of the fragment containing "a", such that the packet is received by the NIDS, but will be discarded before reaching the attack site. In this case, the attack succeeds because the attack site receives "login root" and the NIDS did not detect the attack.

Independent claim 18 recites in relevant part,

A method for normalization of traffic data, received from an internet and transmitted to a local network, said method comprising:

dynamically establishing and maintaining a normalization table in a traffic normalizer, said traffic normalizer being interposed between said internet and said local network;

receiving a packet fragment from said internet at said traffic normalizer, said packet fragment being addressed to an end-system in said local network;

…

if said conflict does not exist, simultaneously transferring said packet fragment to a network intrusion detection system and said end-system of said local network.

Similarly, independent claim 30 recites in relevant part,

A method for normalization of traffic data, received from an internet and transmitted to a local network, said method comprising:

dynamically establishing and maintaining a normalization table in a traffic normalizer, said traffic normalizer being interposed between said internet and said local network;

receiving a packet fragment from said internet at said traffic normalizer, said packet fragment being addressed to an end-system in said local network;

…

if said packet fragment does fit said sliding bit-mask, simultaneously transferring said packet fragment to a network intrusion detection system and said end-system of said local network.

Similarly, independent claim 37 recites in relevant part,

A programmable storage device readable by machine, tangibly embodying a program of instructions executable by said machine to perform a method for normalization of traffic data,

received from an internet and transmitted to a local network, said programmable storage device comprising instruction for:

dynamically establishing and maintaining a normalization table in a traffic normalizer, said traffic normalizer being interposed between said internet and said local network;

receiving a packet fragment from said internet at said traffic normalizer, said packet fragment being addressed to an end-system in said local network;

...

if said packet fragment does fit said sliding bit-mask, simultaneously transferring said packet fragment to a network intrusion detection system and said end-system of said local network.

Nowhere does Vaidya disclose, teach or suggest normalization of traffic data received from an internet and transmitted to a local network as recited in independent claims 18, 30, and 37 of the present invention. Instead Vaidya discloses a dynamic signature-based Network Intrusion Detection System (NIDS) which resides in a local network.

Nowhere does Vaidya disclose, teach or suggest a traffic normalizer being interposed between the internet and the local network as recited in independent claims 18, 30, and 37 of the present invention. Instead Vaidya discloses a dynamic signature-based Network Intrusion Detection System (NIDS) which resides in a local network.

Nowhere does Vaidya disclose, teach or suggest receiving a packet fragment from the internet, where the packet fragment is addressed to an end-system of the internet as recited in independent claims 18, 30, and 37 of the present invention. Instead Vaidya discloses the use of headers of a complete packet.

Nowhere does Vaidya disclose, teach or suggest transferring the packet fragment to a network intrusion detection system and the end-system of the local network. Instead Vaidya discloses the use of headers of a complete packet.

For at least the reasons outlined above, Applicants respectfully submit that Vaidya does

disclose, teach or suggest every feature recited in independent claims 18, 30, and 37 of the present invention.

B. The Spiegel Reference

Spiegel discloses a system that updates a file by making a backup copy of a portion of the file that includes changed data. Through cross-linking of certain storage areas, called units, the revised segment of the file is related to the other file portions. (col. 2, lines 48-52).

The Office Action cites col. 5, lines 44-47, which read "Further to a unit's composition, replacement data 74 may be provided to replace header information, especially where data is moved from one location to another and where the unit has been used during an update."

Spiegel's memory storage areas, called units, for files or segments of files and the replacing of header information of files or segments of files is not analogous to the features of the present invention.

Nowhere does Spiegel disclose, teach or suggest normalization of traffic data received from the internet and transmitted to a local network as recited in independent claims 18, 30, and 37 of the present invention. Instead Spiegel discloses a file updating system.

Nowhere does Spiegel disclose, teach or suggest a traffic normalizer being interposed between the internet and the local network as recited in independent claims 18, 30, and 37 of the present invention. Instead Spiegel discloses a file updating system.

Nowhere does Spiegel disclose, teach or suggest receiving a packet fragment from the internet, where the packet fragment is addressed to an end-system of the internet as recited in independent claims 18, 30, and 37 of the present invention. Instead, Spiegel discloses sending and receiving of complete packets, comprising files or portions of files.

Nowhere does Spiegel disclose, teach or suggest transferring the packet fragment to a network intrusion detection system and the end-system of the local network. Instead, Spiegel discloses sending and receiving of complete packets, comprising files or portions of files.

As outlined above, Vaidya does not disclose, teach or suggest every feature recited in

independent claims 18, 30, and 37. Spiegel does not cure the deficiencies of Vaidya. Accordingly, Vaidya and Spiegel, either independently or in combination would not have rendered obvious the subject matter of independent claims 18, 30, and 37 and dependent claims 19-25, 34-36, and 38 under 35 U.S.C. §103(a). Withdrawal of the rejection of pending claims 18-25, 30, and 34-38 is respectfully solicited.

II. Formal Matters and Conclusion

Claims 18-25, 30, and 34-38 are pending in the present application. The claims have been amended, above, to overcome the rejection. In view of the foregoing, the Examiner is respectfully requested to reconsider and withdraw the rejection to the claims. In view of the foregoing, Applicants submit that claims 18-25, 30, and 34-38 are patentably distinct from the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary.

Please charge any deficiencies and credit any overpayments to Attorney's Deposit Account Number 50-0510.

Respectfully submitted,

Dated: September 14, 2007

/Peter A. Balnave/
Peter A. Balnave, Ph.D.
Reg. No. 46,199

Gibb & Rahman, LLC
2568-A Riva Road
Suite 304
Voice: (410) 573-5255
Fax: (301) 261-8825
Annapolis, MD 21401
Customer Number: 29154